Simplifying Security and PSA Compliance

NXM **TrustStar**™ is the first chip vendor agnostic platform that orchestrates the design, deployment, and management of PSA security at scale across the entire IoT supply chain. TrustStar offers a unified software platform that reduces the complexity of managing a chain-of-trust, replacing proprietary tools and manual processes with a fully automated solution.

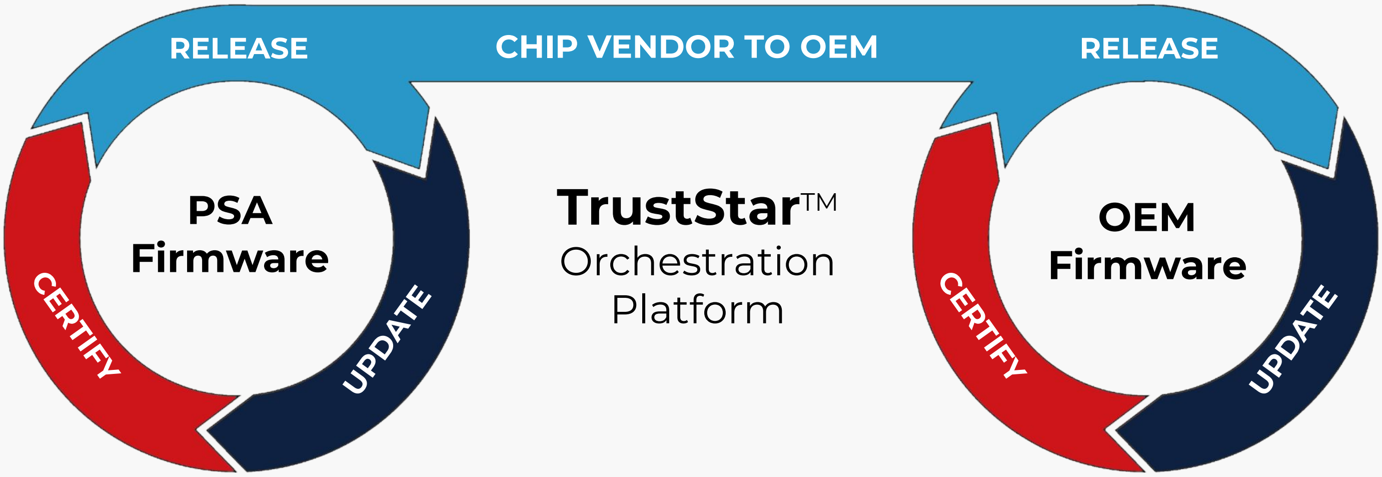
The best part is no part

Coordinating the supply chain to maintain security has historically been a complex, labor intensive undertaking involving just in time delivery of specialized modules (HSMs) for securing production processes. TrustStar replaces this with a secure, auditable, software-based Distributed Ledger Technology (DLT) process that not only protects the entire supply chain but eliminates single points-of-failure vulnerabilities that can lead to catastrophic, network-wide device breaches.

What is PSA?

Originally spearheaded by Arm, Platform Security Architecture (PSA) is an open framework that seeks to standardize security in connected devices through adoption of a common security API anchored in silicon, allowing the industry to transition from vendor-specific implementations to a global standard. PSA focuses on low-level chip features, including secure boot, crypto libraries and secure storage.

The Big Picture



CHIP VENDOR PROCESS	
UPDATE	Chip vendor updates PSA component firmware
CERTIFY	Lab tests, certifies, then registers firmware with TrustStar
RELEASE	Chip vendor releases PSA firmware to OEM

OEM PROCESS	
UPDATE	OEM updates product firmware
CERTIFY	Lab tests, certifies, then registers firmware with TrustStar.
RELEASE	OEM releases product firmware to TrustStar, pushes image to installed devices.

Why does the PSA supply chain require orchestration?

The steps needed to create production-ready PSA-certified chips requires complex coordination between multiple stakeholders. TrustStar orchestrates the entire product supply chain process, including PSA chip certification, flashing, product manufacturing and ongoing firmware updates, automatically tracking and validating every step as the chip passes through the supply chain.

Cost-effective solution for the entire supply chain

In the same way that PSA replaces vendor-specific security on a chip, TrustStar eliminates multi-vendor fragmentation, making it easier for chip vendors, contract manufacturers and OEMs to quickly release and ramp production of new products that meet the security needs of today's market.

Fast-Track to UL's Secure IoT Component Qualification

TrustStar enables manufacturers to reuse their PSA certification and reduce overheads and costs associated with third-party evaluations such as UL's *Secure IoT Component Qualification* certification.

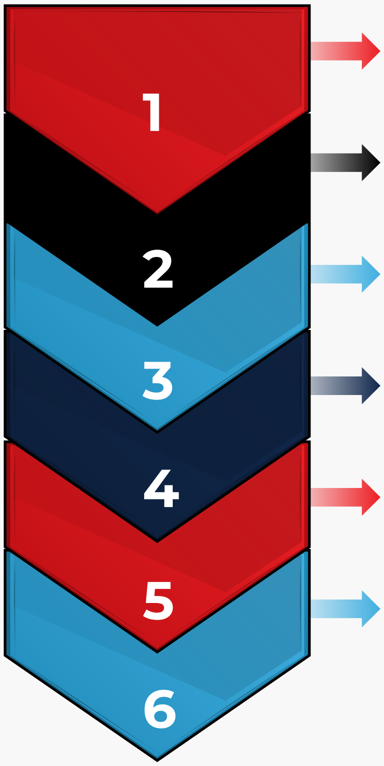
Eliminates device cloning and firmware piracy

With TrustStar's optional on-prem solution for contract manufacturers, OEMs gain greater control over the manufacturing process and unwanted grey market activities. This includes the ability to control how many products are manufactured, as well as preventing cloning and firmware piracy.

Compatible with major IoT platforms

TrustStar is cloud agnostic and works with leading platform vendor solutions that provide device management tools and services for IoT products, including AWS IoT Core and Microsoft Azure IoT Hub.

Secure Supply Chain Management



1. Rapid PSA Chip Certification

- PSA certification records are automatically uploaded to the TrustStar platform
- Integrates PSA certification as part of the firmware amd product release process

2. Volume PSA Chip flashing

- On-premise solution gives chip manufacturers ability to flash PSA chips at volume
- Integrates with high-volume flashing equipment to inject PSA certified firmware
- Automatically uploads PSA chip identity and public key to TrustStar

3. Managed Contract Manufacturing

- Optional on-prem solution for contract manufacturers
- Ability to control how many products a contract manufacturer can build
- Ability to prevent device cloning and firmware piracy

4. Product-level Certification

- Integrates 3rd-party product certification in the firmware release process
- Minimizes security downtime when a firmware update is urgently required
- Automatically uploads certification records to TrustStar

5. Firmware Management

- TrustStar includes developer tools for registering firmware releases
- Automatically monitors the breakdown of firmware versions deployed in the field

6. IoT Platform Integration

- Integrates with popular IoT management platforms (e.g. AWS IoT Core, Azure IoT Hub, etc.)
- Ability to push firmware updates to OEM products